approved processes and that a host computer is programmed to decrypt the encrypted data in the registry file and then search that decrypted data for an entry matching an identifier that identifies a starting process to be executed. As will be shown in detail below, the last of the three basic criteria for establishing a *prima facie* case of obviousness, namely, that the combined prior art references must teach or suggest all the claim limitations, has not been met by the Final Rejection. Accordingly, the Applicant believes that the rejection based on Hiyama, McGee and Hile should be withdrawn.

In particular, the Examiner asserts that McGee teaches the encryption and decryption of registry information, citing column 4, lines 35-39, which reads as follows:

> For integrity purposes, the application registration data may <u>optionally</u> be digitally signed by, for example, a user's own private signing key . . . .

(Emphasis added.) The Applicant respectfully submits, however, that this "option" applies only in the case when different users are approved to execute different files. Digitally signing registration data using a "user's own private signing key" clearly implies that the registration data is personal to that user.

In contrast, Applicant's claims 1 and 30 each recite that the "registry file contain[s] encrypted data representing a list of <u>all processes</u> that are <u>approved</u> by the system manufacturer or service provider to run on the imaging system". (Emphases added.)

Furthermore, McGee discloses that conventional digital signing techniques can be used to sign the application registration data, "such as generating a hash value of the application registration data and digitally signing the hash value using the private signing key". [McGee, col. 7, lines 5-9.] However, the application registration data itself comprises a list of hash values of approved applications. [McGee, col. 5, lines 13 and 14.] More precisely, each hash value in the registry is generated from the executable file corresponding to the application. [McGee, col. 6, lines 54-56.] Accordingly, the digital signature of McGee is an encryption of a hash value derived from a list of hash values generated from the executable files. Conversely, the decryption of that digital signature will be the hash value derived from the list (i.e., multiplicity) of hash values and is not the hash value of any particular executable file.

Moreover, the optional verification of the digital signature, as taught by McGee, "may occur once at the time a user initially logs in, each time this data is utilized, or at any other convenient frequency." [McGee, col. 7, lines 60-62.] The purpose of the digital signature verification is to "determine if the application registration data is valid by checking its integrity". [McGee, col. 7, lines 49-53.] Thus, the digital signing taught by McGee is for the purpose of verifying the data in the personal registry file of a particular user, and not for the purpose of verifying that the file to be executed on a particular system has been approved for execution on that system.

For the purpose of verifying that the file to be executed on a particular system has been approved for execution on that system, McGee teaches using hash values of those executable files. More specifically, McGee teaches that the execution of files is monitored by comparing the hash values stored in the registry list to the hash value generated from the file to be executed. [McGee, col. 4, lines 25-27.] If there is a match, the application is granted execution privileges. [McGee, col. 5, lines 6-7.]

More specifically, McGee uses hash values generated using "one-way hash functions", as stated in column 7 at line 28 and in column 8 at line 53. A hash function H is a transformation that takes a variable-size input m and returns a fixed-size string, which is called the hash value h (that is $h = H(m)$. One basic requirement of a cryptographic hash function is that it be "one-way". A hash function is said to be "one-way" if it is hard to invert, meaning that given a hash value h, it is computationally unfeasible to find some input x such that $H(x) = h$. In other words, the one-way hash values disclosed by McGee are not decrypted and could not be decrypted, which is largely due to the fact that the hash values are generated by transforming a large domain into a small range, resulting in lost data that cannot be recovered by inverting the hash function.

In contrast, Applicant's claims 1 and 30 each recite that the host computer is programmed to search the decrypted data "for an entry matching the identifier received from said operating system identifying a starting process of said application program to be executed by said operating system". The hash values generated from executable files in accordance with the McGee teaching correspond to Applicant's identifiers. These hash values exist in the registry of McGee in un-encrypted form, separate and apart from the digital signature, which is an encryption derived from those hash values. Since McGee's identifiers are not encrypted, they do not need to be decrypted. Accordingly, the search of those hash values (i.e., identifiers) for a hash value identifying the file to be executed does not constitute a search of "decrypted data", as recited in Applicant's claims 1 and 30.

Accordingly, the rejection of claims 1 and 30 based on Hiyama in view of McGee and Hile does not satisfy the requirement that the cited prior art disclose all of the limitations of the rejected claim.

The obviousness rejections set forth in ¶¶ 4 and 5 of the action are both based on Hiyama, McGee and Hile as applied to claim 1 and/or 30 in combination with a fourth reference (Yamamoto and Kisor). These rejections suffer from the same infirmities as those noted above vis-à-vis the Hiyama/McGee/Hile combination. Accordingly, it is believed that claims 2, 3, 5, 10 and 33 are patentable at least for the same reasons that claims 1 and 30, on which they depend, are patentable.

In view of the foregoing, the Applicant submits that this application is now in condition for allowance. Reconsideration of the application and allowance of claims 1-5, 8-13, and 30-36 are hereby requested.

Respectfully submitted,

Dennis Flaherty

July 22, 2005
Date

Dennis M. Flaherty
Reg. No. 31,159
Ostrager Chong Flaherty &
Broitman P.C.
250 Park Avenue, Suite 825
New York, NY 10177-0899
Tel. No.: 212-681-0600

CERTIFICATE OF MAILING

The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date set forth below.

July 22, 2005

Dennis Flaherty

Dennis M. Flaherty